

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-296978

(43)公開日 平成11年(1999)10月29日

(51)Int.Cl. ⁸	識別記号	F I	
G 1 1 B 20/10		G 1 1 B 20/10	H
G 0 9 C 5/00		G 0 9 C 5/00	
G 1 1 B 20/12	1 0 2	G 1 1 B 20/12	1 0 2

審査請求 未請求 請求項の数5 OL (全 11 頁)

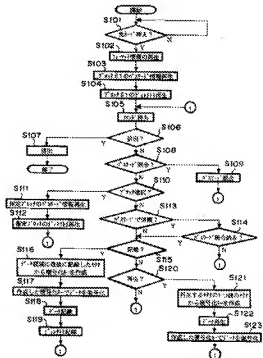
(21) 出願番号	特願平10-93276	(71) 出願人	000001007 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
(22) 出願日	平成10年(1998) 4月6日	(72) 発明者	田中 玄和 東京都大田区下丸子3丁目30番2号 キヤ ノン株式会社内
		(74) 代理人	弁理士 山下 穰平

(54) 【発明の名称】 情報記録再生装置

(57) 【總約】

【課題】 ファイルごとに暗号化／復号化しているので、1つのキーが特定されてしまうとファイル全体が解読されてしまう。

【解決手段】 セクタごとにこれから記録／再生するセクタから所定の数だけ前のセクタに記録されているデータをもとに暗号化キー／復号化キーを作成する。また、所定の数をファイルのディレクトリに記録し、ファイルごとに所定の数を異ならせる。



【特許請求の範囲】

【請求項1】 1つまたは複数のセクタより成る複数のトラックを有する追記型記録媒体にデータを記録／再生する手段と、前記記録媒体にデータを管理するためのディレクトリを記録／再生する手段と、データの記録前にデータを暗号化する手段と、再生されたデータを復号化する手段とを有する情報記録再生装置において、前記記録媒体に既に記録されているデータをもとにデータを暗号化／復号化するための暗号化キー／復号化キーを作成する手段を備え、前記暗号化キー／復号化キー作成手段はセクタごとにこれから記録／再生するセクタから所定の数だけ前のセクタに記録されているデータをもとに暗号化キー／復号化キーを作成することを特徴とする情報記録再生装置。

【請求項2】 前記暗号化キー／復号化キー作成手段は、前記所定の数だけ前のセクタにデータが記録されていないときは、予め決められたデフォルト値をもとに暗号化キー／復号化キーを作成することを特徴とする請求項1に記載の情報記録再生装置。

【請求項3】 前記所定の数をもとに前記ディレクトリに記録しておくことを特徴とする請求項1に記載の情報記録再生装置。

【請求項4】 前記記録媒体のファイルごとに前記ディレクトリに記録する所定の数を変えさせることを特徴とする請求項3に記載の情報記録再生装置。

【請求項5】 前記記録媒体は、光カードであることを特徴とする請求項1に記載の情報記録再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報記録媒体に情報を記録／再生する情報記録再生装置に関し、特にデータの暗号化／復号化に関するものである。

【0002】

【従来の技術】従来、光学的に情報を記録し、あるいは記録された情報を読み出す媒体の形態として、ディスク状、カード状、テープ状等各種のものが知られている。これらの媒体のうち、カード状に形成された光学的情報記録媒体（以下光カードと称する）は、磁気カードと比較して数千倍〜一万倍の記録容量を有し、光ディスクと同様に書き換えはできないが、その記録容量が1〜6Mバイトと大きいことから銀行の預金通帳、携帯用の地図、あるいは買い物等に用いるプリペイドカード等として広い応用範囲が考えられている。

【0003】このような光カードにデータを記録、再生する場合、通常は、データと共にデータを管理するためのディレクトリを光カードの一部に記録して、データをファイルごとに管理するのが一般的である。ディレクトリは図3に示すようにファイル名、先頭データの開始アドレス、連続して記録したセクタ数等のファイル管理に必要な情報から成っている。このディレクトリはデータ

を記録する際にデータの管理情報として光カードの記録領域の一部に記録される。

【0004】図4は光カードの概略平面図で、1は光カード、2は情報記録領域である。情報記録領域2内にはトラッキングトラック31〜3n+1が一定間隔を置いて平行に配列され、その各トラッキングトラックの間に情報を記録するための情報トラック41〜4nが設けられている。各情報トラックの両端には情報トラックを識別するための物理トラッキングナンバー51〜5nが予め付加されている。また、図4の光カードでは、情報トラック42〜4kをブロック61、情報トラック4k+1〜4n-1をブロック62として、情報記録領域2が2つのブロックに分割されている。光カード1を複数のブロックに分割することに關しては特開昭63-244385号公報に記載されている。

【0005】例えば、光カードを医療情報記録用の媒体として用い、これにある患者の心電図情報と血圧情報を記録する時は、ブロック61に心電図情報を、ブロック62に血圧情報を記録することが可能である。このように記録するデータの種類のごとにブロック分けを行った場合、心電図情報を再生する時はブロック61内のデータだけを再生すればよいために、アクセス時間を短縮することができる。もちろん、ブロックの分割数やブロック内の情報トラック数は記録するデータの種類やデータ量に応じて任意に設定することができる。

【0006】また、光カード1においては、ブロックごとに1本の情報トラックのセクタ数とセクタサイズを変える方式が知られている。図5は1本の情報トラックに記録するデータのセクタサイズとセクタ数の関係の例を示している。図5において、セクタタイプ1は1024バイトのセクタを情報トラック4に1個記録し、セクタタイプ2は512バイトのセクタを情報トラック4に2個記録し、セクタタイプ3は256バイトのセクタを情報トラック4に4個記録し、セクタタイプ4は128バイトのセクタを情報トラック4に6個記録し、セクタタイプ5は64バイトのセクタを情報トラック4に8個記録し、セクタタイプ6は32バイトのセクタを情報トラック4に12個記録する事を示している。

【0007】このような方式で、例えば768バイトのデータをセクタタイプ1で記録する場合は、1セクタ（情報トラック1本）を記録するだけでよいが、セクタタイプ6で記録すると、24セクタ（情報トラック2本）を記録しなければならない。そのため、セクタタイプ6で記録した場合は時間がかかるばかりでなく、光カードの記録容量を無駄にしてしまう。また、32バイトのデータをセクタタイプ1で記録する場合は、1本の情報トラックを使ってしまうが、セクタタイプ6で記録すると、1セクタで済み、セクタタイプ1に比べて1/12の情報トラックしか使わない。このように記録するデータサイズに応じてセクタタイプを選択することによ

り、アクセス速度を早くできるばかりでなく、光カードの記録領域を有効に使用することができる。

【0008】ここで、図4において、711～711はブロック61内に記録されているデータ、721～721はブロック62内に記録されているデータである。811～811はブロック61内に記録されているデータ71を管理するためのディレクトリ、821～821はブロック62内に記録されているデータ72を管理するためのディレクトリである。データはB方向に追記し、ディレクトリはF方向に追記していく。前述のように光カードに医療情報を記録する場合は、心電図情報をデータ71、その管理情報をディレクトリ81、血圧情報を72、その管理情報を82として記録すればよい。

【0009】また、心電図情報のようにデータ量の大きな情報を記録する場合は、データ711～711のようにセクタサイズを大きくし、1本の情報トラックに記録するセクタ数を1にすると、アクセス速度を早めることができる。逆に、血圧情報のようにデータ量が小さい場合は、データ721～721のようにセクタサイズを小さくし、1本の情報トラックに記録するセクタ数を多くすれば、光カードの記録容量を有効に使用することができる。なお、ディレクトリのデータサイズは比較的小さいので、例えばセクタタイプ5で記録するのがよい。

【0010】更に、光カードのいずれのブロックにも属さない情報トラック41と情報トラック4nには、上述した光カード1のブロック分割数、各ブロックのトラック本数、各ブロックで使用するセクタタイプ等の光カード管理情報9（以下、フォーマット情報と称する）が記録されている。図6はこのフォーマット情報の内容を示す図で、先頭の識別情報はフォーマット情報であることを示す情報であり、例えばASCIIコードで“FM T”といった情報が記録される。次のブロック分割数は光カード1がいくつかのブロックに分割されているかを示す情報である。次に、ブロック61～ブロック6nの各情報トラック数とセクタタイプを示す情報が記録されている。

【0011】ところで、光カードの情報の記録や再生は任意の利用者が行うことが可能である。そのため、多数の利用者が使用することにより誤って必要な情報を破壊してしまったり、故意に情報を改ざんしたり、あるいは機密性の高い情報を他人に見られてしまう可能性がある。そこで、光カード1のブロックごとに個人固有の情報（以下パスワード情報と称する）を記録しておき、パスワード情報が記録されているブロック内にデータを記録または再生する時は、パスワード情報を入力し、入力したパスワード情報とブロック内に記録されているパスワード情報とを照合し、照合結果が一致した時のみブロック内の情報の記録再生を許可するという方法が採用されている。

【0012】図4の1011と1012はブロック61のバ

スワード情報である。このパスワード情報は、図7に示すように識別情報とパスワード情報から構成されている。識別情報はパスワード情報であることを示す情報で、例えば、ASCIIコードで“PWD”といった情報が用いられる。次に、実際のパスワード情報が記録される。このようなパスワード情報を用いることにより、例えば、心電図情報を記録再生する場合は、ホストコンピュータからパスワード情報を入力し、これがブロック61内のパスワード情報と一致した時のみ心電図情報のアクセスが可能となる。これに対して、ブロック62内のパスワードを記録するトラック4k+1、4n-1にはパスワード情報が記録されていないため、自由に血圧情報の記録再生が可能である。

【0013】しかし、光カードに情報を記録する場合は、微小スポット状に絞られた光ビームを記録情報に従って変調し、変調された光ビームを情報トラック上にスキャンすることにより、光学的に検出可能なビット列として記録するので、パスワードでブロック6内のアクセスを制限しても、光学顕微鏡等を用いて解析されると機密性の高い情報が他人に見られてしまう可能性がある。そこで、更にセキュリティを高めるために、光カードに記録するデータを暗号化キーにより暗号化して記録し、再生時は暗号化されたデータを復号化キーにより復号化して再生する方法が提案されている。

【0014】この方式を用いることにより、光カードに記録されたデータを光学顕微鏡等によって解析された場合でも、解析したデータが意味をなさないものとなり、光カードに記録されたデータの機密性を保つことが出来る。光カードに記録するデータを暗号化する方式としては、様々な方式が考えられ、公開鍵方式のRSA暗号や共通鍵方式のDES暗号などが有名であるが、ここでは、説明を簡単にするためにシーザ暗号を例に説明する。シーザ暗号ではアルファベットに数をA=0、B=1、…、Z=25と対応させ、平文の1文字を表す数をx、暗号文の1文字を表す数をc、暗号化キーを表す数をkとおくと、

$$c = (x + k) \bmod 26$$

の関係式で表される暗号方式である。但し、 $a \bmod n$ はaをnで割った余りを示す。また、暗号文を平文にする復号化の場合は、

$$x = (c - k) \bmod 26$$

の関係式で表される。従って、シーザ暗号では暗号化キーと復号化キーは同じキーとなる。そして、例えば暗号化キーkが1の場合は、平文が“ABC”であれば暗号文は“BCD”と暗号化される。しかしながら、このままではアルファベットの文字しか扱えないので、暗号化の式を、

$$c = (x + k) \bmod 256$$

の様に拡張し、また復号化の式を、

$$x = (c - k) \bmod 256$$

の様に拡張することにより、1バイトで表される全ての文字を扱うことが可能となる。そして、これらの暗号化または復号化は高速で実行する事が望ましいために、ハードウェアで行うのが一般的である。

【0015】次に、暗号化キーの作成方法について説明する。暗号化キーの作成方法は様々な方法が考えられるが、例えば光カードに記録されているフォーマット情報、パスワード情報、ディレクトリ等の情報のある関数に入力する事により暗号化キーを作成できる。従って、暗号化キーを k 、キーを作成するための暗証番号を n とすると、

$$k = F(n)$$

の関係式がなりたつ。但し、関数 $F(n)$ は暗号化キーを作成する関数であり、圧縮関数等を用いられる。圧縮関数とは、任意のビット長のビット列にある長さのビット列に変換する関数である。光カード情報記録再生装置はこの暗号化キーを用いてデータの暗号化、暗号化されたデータの復号化を行う。

【0016】次に、光カードに情報を記録または再生する光カード情報記録再生装置について説明する。図8は光カード情報記録再生装置の概略構成を示すブロック図である。図8において、31は光カード1に情報を記録、再生する光カード情報記録再生装置であり、上位制御装置のホストコンピュータ32に接続されている。情報記録再生装置31はホストコンピュータ32の制御に基づいて情報の記録、再生を行う。37は不図示の搬送機構を駆動して光カード1を情報記録再生装置31内の所定位置に導入し、また、所定位置にて光カード1をR方向に往復移動させ、更に光カード1を機外に排出するためのカード送りモータである。38は光源の半導体レーザを含む光ビーム照射光学系であり、情報の記録、再生時には光源の光ビームを微小光スポットに絞って光カード1上に照射する。

【0017】また、39は光カード1から反射された光を検出する光検出器、40は光ビーム照射光学系38の一部を駆動して光カード1面上の光スポットのピント位置をZ方向、即ち光カード面と垂直方向に移動させてオートフォーカス制御を行うためのAFアクチュエータ、41は光ビーム照射光学系38の一部を駆動して光カード1面上の光スポットをY方向、即ち光カードの情報トラックに直交する方向に移動させてオートトラッキング制御を行うためのATアクチュエータである。これらの光ビーム照射光学系38、光検出器39、AFアクチュエータ40、ATアクチュエータ41を含んで光ヘッド30が構成されている。36は光ヘッド50をY方向に移動させて光スポットを所望のトラックにアクセスするためのヘッド送りモータである。

【0018】MPU33は情報記録再生装置31内の各部を制御するためのプロセッサ回路であってROM、RAMを内蔵している。MPU33はカード送りモータ3

6、カード送りモータ37などを制御し、また、ホストコンピュータ32とデータの送受信を行う。AT/AF制御回路34は光検出器39からの出力信号からAT/AF制御信号を検出し、それに基づいてAFアクチュエータ40とATアクチュエータ41を駆動し、光ビーム照射光学系38からの光スポットがカード面に焦点を結ぶように、光スポットが情報トラックに追従して走査するようにオートフォーカス制御とオートトラッキング制御を行う。

【0019】変復調回路35はMPU33の制御に基づいて記録データを変調し、再生データを復調するための回路、暗号化/復号化回路42は記録データを暗号化し、再生データを復号化するための回路である。情報の記録時には、ホストコンピュータ32からMPU33に記録データが転送され、その後、暗号化/復号化回路42で記録データが暗号化される。変復調回路35では暗号化されたデータを変調し、変調信号に従って光ビーム照射光学系38内の光源を駆動し、この変調された光源の光ビームを光カード1の情報トラックに走査することによって情報の記録を行う。

【0020】一方、情報の再生時には、光ビーム照射光学系38から再生用光ビームを光カード1の情報トラックに走査し、光検出器39で光カード1からの反射光を検出する。このとき、変復調回路35は光検出器39の出力信号から情報再生信号を生成し、再生信号の復調を行う。復調されたデータはMPU33のRAMに蓄えられ、その後、暗号化/復号化回路42によって暗号化されたデータが復号化される。復号化されたデータはMPU33からホストコンピュータ32に転送される。ホストコンピュータ32は情報記録再生装置31とコマンドやデータの送受信を行い、セクタごとに情報の記録や再生を行う。

【0021】次に、光カード情報記録再生装置において光カードのデータにアクセスする際の動作について図9を参照して説明する。図9において、まず、情報記録再生装置31は光カード1が挿入されたかを監視している(901)。光カードが挿入されると、最初にフォーマット情報9を再生する(902)。フォーマット情報を再生すると、光カード1の記録領域がどのように分割されているかが分かる。この場合、フォーマット情報に基づいてデフォルトのブロックとしてブロック61が自動的に選択され、ブロック61のパスワード情報10が再生される(903)。パスワード情報はMPU33内のRAMに記憶し、もし、パスワードが記録されていなかったらこのブロックがパスワードで保護されていないことをRAMに記憶しておく。

【0022】次に、ブロック61のディレクトリ81を順次再生し、MPU33内のRAMに読み込んだ順に記憶する(904)。光カード1には、データもディレクトリもシーケンシャルに記録されているので、ディ

レクトリを再生すると、再生したディレクトリの数と、再生したディレクトリの内容から、ディレクトリの記録開始位置とデータの記録開始位置がわかる。このようにして光カード情報記録再生装置31はホストコンピュータ32からのコマンドを待つ状態となり(5905)、コマンドの種類に応じて以下の処理を実行する。まず、コマンドが排出コマンドであるかをチェックする(5906)。コマンドが排出コマンドであった場合は、光カード1の排出を実行し、この光カード1に対する処理を終了する(5907)。

【0023】一方、コマンドが排出コマンドでなかった場合は、パスワード照合コマンドであるかどうかをチェックし(5908)、もし、パスワード照合コマンドであった場合は、パスワードの照合を行う(5909)。即ち、5903で再生してRAMに記憶しておいたパスワードと、パスワード照合コマンドによってホストコンピュータ32から送られてきたパスワードを照合する。ここで、もし両方のパスワードが一致した場合は、ブロック61におけるパスワードが照合済みであることをMPU33内のRAMに記憶しておく。パスワードが一致しなかった場合は、そのまま5905のコマンド待ち処理に移行する。また、現在選択されているブロックがパスワードで保護されていないときは、照合は行わず、5905に戻る。

【0024】パスワードの照合処理を終了すると、コマンドがブロック選択コマンドであるかをチェックし(5910)、ブロック選択コマンドであった場合は、5902で再生したフォーマット情報に基づいて指定されたブロックのパスワード情報を再生する(5911)。再生したパスワード情報は5903と同様にMPU内のRAMに記憶しておく。次いで、指定されたブロックに記録されているディレクトリをすべて再生し(5912)、MPU33内のRAMに読み込んだ順に記憶し、ブロック選択の処理を終了する。

【0025】一方、5910でコマンドがブロック選択コマンドでなかった場合は、コマンドは記録コマンドか再生コマンドであり、現在選択されているブロックがパスワードで保護されている場合は、パスワードが照合済みか確かめなければならないので、まず、パスワードで保護されているか調べ(5913)、保護されている場合はパスワードが照合済みかをチェックする(5914)。このチェックは、5909でRAMに記憶しておいた情報を参照することによって行う。パスワードが照合済みでない場合は、5905に戻る。パスワードが照合済みの場合、及び5913においてパスワードで保護されていないと判断された場合は、次の5915の処理に移行する。

【0026】5915においては、コマンドが記録コマンドであるかをチェックし、記録コマンドであった場合は、暗号化に必要な暗号化キーを作成する(591

6)。暗号化キーは、RAMに記憶されている最後のディレクトリを基に作成する。このディレクトリは、現在アクセスしているブロックに最後に記録されたディレクトリである。このブロックに初めて記録するデータである場合は、また、このブロックにはディレクトリは記録されていないので、予め決められたデフォルトの値を基に暗号化キーを作成する。暗号化キーの作成には、前述のような圧縮関数を用いられる。

【0027】次いで、記録コマンドと共にホストコンピュータ32から送られてきたデータを5916でディレクトリから作成した暗号化キーによって暗号化し(5917)、暗号化されたデータを現在選択されているブロックの記録を開始すべき位置から記録する(5918)。その後、記録したデータを管理するためのディレクトリを記録し、RAMにも同様のディレクトリを記憶して(5919)、記録コマンドの処理を終了する。

【0028】一方、5915で記録コマンドでなかった場合は、コマンドが再生コマンドであるかをチェックする(5920)。再生コマンドでない場合は、情報記録再生装置31がサポートしないコマンドなので、5905に戻り、再生コマンドであった場合は、復号化キーを作成する(5921)。復号化キーはRAMに記憶されているディレクトリから再生すべきデータのディレクトリをサーチし、そのディレクトリの1つ前のディレクトリを基に作成する。1つ前のディレクトリが無い場合は、予め決められたデフォルトの値を基に復号化キーを作成する。次いで記録コマンドで指定されたファイル名と、RAMに記憶しているディレクトリから再生すべきセクタアドレスを求め、データを再生する(5922)。ここで再生したデータは、暗号化されたデータであるので、作成した復号化キーを用いて復号化し(5923)、復号化したデータをホストコンピュータ32に転送して再生処理を終了する。

【0029】

【発明が解決しようとする課題】従来の方法では、最後に記録したファイルのディレクトリから暗号化キーを作成し、再生するファイルの1つ前のファイルのディレクトリから復号化キーを作成している。即ち、ファイルごとに暗号化/復号化しているので、1つのキーが特定されてしまうと、ファイル全体が解読されてしまい、セキュリティが低いという問題点があった。

【0030】本発明は、上記従来の問題点に鑑み、セクタごとに暗号化キー/復号化キーを異ならせることにより、更にセキュリティを向上することが可能な情報記録再生装置を提供することを目的とする。

【0031】

【課題を解決するための手段】本発明の目的は、1つまたは複数のセクタより成る複数のトラックを有する追記型記録媒体にデータを記録/再生する手段と、前記記録媒体にデータを管理するためのディレクトリを記録/再

生する手段と、データの記録前にデータを暗号化する手段と、再生されたデータを復号化する手段とを有する情報記録再生装置において、前記記録媒体に既に記録されているデータをもとにデータを暗号化／復号化するための暗号化キー／復号化キーを作成する手段を備え、前記暗号化キー／復号化キーを作成手段はセクタごとにこれから記録／再生するセクタから所定の数だけ前のセクタに記録されているデータをもとに暗号化キー／復号化キーを作成することを特徴とする情報記録再生装置によって達成される。

【0032】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。まず、本発明の第1の実施形態について説明する。第1の実施形態による情報記録再生装置のハードウェアの構成は図8と同様の構成とし、記録媒体としては図4の光カードを用いるものとする。また、光カード1に記録するファイルデータを管理するためのディレクトリは図3、セクタタイプは図5、フォーマット情報は図6、パスワード情報は図7のものを用いるものとする。これらの図8、図4、図3、図5、図6、図7については先に述べたので詳しい説明を省略する。

【0033】図1は本実施形態の動作を示すフローチャートである。なお、図1のS101～S115は従来の動作を示す図9のS901～S915と同じであるので簡単に説明する。図9において、まず、S101で情報記録再生装置31に光カード1が挿入されると、光カード1のフォーマット情報を再生する(S102)。フォーマット情報を再生すると、光カード1のブロックの分割状態が分かり、本実施形態では従来と同様にデフォルトのブロックとしてブロック61を自動的に選択し、ブロック61のパスワードを確認する(S103)。パスワード情報はMPU33内のRAMに記憶しておく。もし、パスワード情報が記録されていなかったときはこのブロックがパスワードで保護されていないことをRAMに記憶しておく。

【0034】次いで、ブロック61のディレクトリ81を順次再生し(S104)、MPU33内のRAMに読み込んだ順に記憶し、光カードにはデータもディレクトリもシーケンシャルに記録されているので、再生したディレクトリの数と内容からディレクトリの記録開始位置とデータの記録開始位置が得られる。次に、情報記録再生装置31はホストコンピュータ32からのコマンドを待ち(S105)、コマンドの種類に応じて以下の処理を実行する。まず、コマンドが排出コマンドであるかをチェックし(S106)、コマンドが排出コマンドであれば光カード1を排出し、この光カードに対する処理を終了する(S107)。排出コマンドでなかったときは、パスワード照合コマンドであるかをチェック(S108)、パスワード照合コマンドであったときはパス

ワードの照合を行う(S109)。即ち、RAMに記憶しておいたパスワードとパスワード照合コマンドによってホストコンピュータ22から送られてきたパスワードを照合し、両方のパスワードが一致すると、ブロック61におけるパスワードが照合済みであることをMPU33内のRAMに記憶しておく。パスワードが一致しなかったときは、S105のコマンド待ち処理に移行する。

【0035】一方、S108でパスワード照合コマンドでなかったときはブロック選択コマンドであるかをチェックし(S110)。ブロック選択コマンドであれば、S102で再生したフォーマット情報に基づいて指定されたブロックのパスワード情報を再生する(S111)。パスワード情報は同様にRAMに記憶しておく。次いで、指定されたブロックのディレクトリを全て再生し(S112)、同様にRAMに読み込んだ順に記憶しブロック選択の処理を終了する。また、ブロック選択コマンドではなかったときはコマンドは記録コマンドか再生コマンドであり、現在選択されているブロックがパスワードで保護されている場合は、パスワードが照合済みか確かめなければならないので、まず、パスワードで保護されているか調べ(S113)、保護されている場合はパスワードが照合済みかをチェックする(S114)。これは、RAMに記憶しておいた情報を参照することによって行う。パスワードが照合済みでなかったときはS105に戻り、パスワードが照合済みの場合、S113でパスワードで保護されていなかったときは次のS115に移行する。

【0036】S115ではコマンドが記録コマンドであるかをチェックし、記録コマンドであった場合は、暗号化に必要な暗号化キーを作成する(S116)。本実施形態では、これから記録するセクタより所定の数だけ前のセクタのデータを暗証番号として暗号化キーを作成し、例えば、ここでは1つ前のセクタのデータから暗号化キーを作成している。また、暗号化キーを作成するための圧縮関数はどのようなものでもよいが、例えば、1つ前のセクタの全てのバイトを排他的論理和で加算した1バイトの値を暗号化キーとする。暗号化キーはMPU33によって作成している。

【0037】従って、MPU33はこれから記録するセクタの1つ前のセクタに記憶されているデータを再生し、そのデータをもとに暗号化キーを作成する。なお、このデータは現在アクセスしているブロックに最後に記録されたデータであり、このブロックに初めてデータを記録する場合は、まだ、このブロックにはデータは記録されていないので、予め決められたデフォルトの値をもとに暗号化キーを作成する。暗号化キーを作成すると、記録コマンドと共にホストコンピュータ32から送られてきたデータを暗号化／復号化回路42によってS116で作成した暗号化キーによって暗号化する(S117)。次いで、暗号化されたデータを現在選択されてい

るブロックの記録開始位置から記録する（S118）。S116からS118の処理は記録するセクタごとに繰り返し行い、セクタごとに1つの前のセクタのデータをもとに暗号化キーを作成し、セクタごとに作成した暗号化キーを用いて暗号化することによって記録していく。その後、記録したデータを管理するディレクトリを記録し、RAMにも同様のディレクトリを記憶して記録コマンドの処理を終了する（S119）。

【0038】次に、S115で記録コマンドでなかったときは、コマンドが再生コマンドであるかチェックし

（S120）、再生コマンドでない場合は、情報記録再生装置31がサポートしないコマンドなのでS105に戻る。再生コマンドであった場合は、復号化キーを作成する（S121）。本実施形態では、復号化キーを作成する場合、再生コマンドで指定されたファイル名と、RAMに記憶しているディレクトリから再生すべきセクタアドレスを求め、次いで再生するセクタの所定の数だけ前のセクタに記録されているデータを再生し、そのデータをもとに復号化キーを作成している。復号化キーはMPU33によって作成し、また、ここでは、例えば再生するセクタの1つ前のセクタに記録されているデータをもとに復号化キーを作成している。1つ前のセクタが無い場合は、予め決められたデフォルトの値を基に復号化キーを作成する。

【0039】復号化キーを作成すると、データを再生し（S122）、ここで再生したデータは暗号化されたデータであるので、暗号化／復号化回路42により作成した復号化キーを用いてデータを復号化し、復号化したデータをホストコンピュータ32に転送する（S123）。S121～S123の処理は再生するセクタごとに繰り返し行い、セクタごとに1つ前のセクタのデータをもとに復号化キーを作成してデータを再生していく。ホストコンピュータ32から指示されたすべてのセクタを再生すると、再びS105に戻ってコマンドを待つ状態となる。

【0040】このように本実施形態では、これから記録／再生するデータの暗号化キー／復号化キーを所定の数だけのセクタに記録されているデータをもとに作成しているので、セクタごとに暗号化キー／復号化キーが異なり、仮にあるセクタの暗号化キー／復号化キーが壊れたとしても、他のセクタを解読することはできず、従来に比べて大幅にセキュリティを高めることができる。更に、暗号化キーや復号化キーを作成するためのデータは暗証番号として記録されたものではないため、暗証番号であるとは気付かれにくく、記録領域が解析されたとしても暗証番号を特定しにくい利点がある。

【0041】次に、本発明の第2の実施形態について説明する。第1の実施形態では暗号化キーと復号化キーを作成する場合、記録または再生するセクタのいくつ前のセクタのデータをもとに作成するかを固定としている

が、本実施形態ではそれをファイルごとに変えている。具体的には、図2のディレクトリを用い、ディレクトリの中にいくつ前のセクタのデータを暗号化キーと復号化キーを作成するかを示す所定の数値を記録しておく。この所定の値は、情報記録再生装置31またはホストコンピュータ32によってファイルごとにデータを作成する際に任意の値を選択して記録するものとする。

【0042】本実施形態の動作は図1と同様であるが、S115で記録コマンドと判断したときは、既にRAMに読み込まれているディレクトリ、即ち、記録するファイルのディレクトリに含まれている所定の値を参照し、記録するセクタより所定の値だけ前のセクタに記録されているデータをもとに暗号化キーを作成する（S116）。次いで、作成した暗号化キーを用いてデータを暗号化し（S117）、光カード1に記録する（S118）。S116～S117の処理はセクタごとに繰り返し行い、セクタごとに記録するセクタより所定の値だけ前のセクタのデータをもとに暗号化キーを作成し、データを記録していく。ホストコンピュータ32から指示されたすべてのセクタを記録すると、記録データを管理するためのディレクトリを記録して（S119）、記録処理を終了する。なお、ファイルを始め記録するときには情報記録再生装置31またはホストコンピュータ32で所定の値を決め、その値を用いて暗号化キーを作成し、ディレクトリを記録するときに所定の値を含むディレクトリを記録する。

【0043】一方、S120で再生コマンドと判断したときはホストコンピュータ32から指定されたファイル名を有するディレクトリ（既にRAMに読み込まれている）に含まれている所定の値を参照し、その値を用いて再生するセクタより所定の値だけ前のセクタに記録されているデータをもとに復号化キーを作成する（S121）。次いで、S122でデータを再生し、S123で復号化キーを用いてデータを復号化する。S121～S123の処理はセクタごとに繰り返し行い、セクタごとに所定の値だけ前のセクタのデータをもとに復号化キーを作成し、データを再生していく。ホストコンピュータ32から指示されたすべてのセクタを再生すると、再びS105に戻ってコマンドを待つ状態となる。

【0044】本実施形態においては、ディレクトリに所定の値を記録し、その値を用いて暗号化キーと復号化キーを作成しているため、暗号化キーと復号化キーを記録または再生するセクタよりいくつ前のセクタのデータをもとに作成するかをファイルごとに変えることができ、第1の実施形態に比べて更にセキュリティを高めることができる。

【0045】なお、以上の実施形態では、暗号化アルゴリズムとしてシーザ暗号を用いているが、DES等の他の暗号化アルゴリズムを用いてもよい。特に、DESはシーザ暗号よりも複雑で解読しにくいので、よりセキュ

リティーを高めることができる。また、情報記録媒体としては光カードに限らず、追記型の記録媒体であればどのような媒体を用いてもよい。

【0046】

【発明の効果】以上説明したように本発明によれば、セクタごとにこれから記録／再生するセクタから所定の数だけ前のセクタのデータをもとに暗号化／復号化キーを作成することにより、セクタごとに異なる暗号化キー／復号化キーを用いてデータを暗号化／復号化することができる。仮に1つのセクタのキーが特定されても、他のセクタは解読することができず、従来に比べてセキュリティを大幅に向上することができる。また、データは暗証番号として記録されたものではないため、暗証番号であるとは気付かれにくく、記録領域が解析されても暗証番号を特定しにくくなり、また、暗証番号をデータとは別にデータ領域に記録する必要はないので、その分記録領域を有効に使用することができる。更に、所定の数をディレクトリに記録し、ファイルごとにその値を異ならせることにより、更にセキュリティを向上することができる。

【図面の簡単な説明】

【図1】本発明による情報記録再生装置の第1の実施形態の動作を示すフローチャートである。

【図2】本発明の第2の実施形態に用いるディレクトリを示す図である。

【図3】従来例のディレクトリを示す図である。

【図4】光カードの例を示す図である。

【図5】セクタタイプの例を示す図である。

【図6】フォーマット情報の例を示す図である。

【図7】パスワード情報の例を示す図である。

【図8】光カード情報記録再生装置の例を示す図である。

【図9】図8の装置の光カードにアクセスする動作を示すフローチャートである。

【符号の説明】

- 1 光カード
- 2 記録領域
- 4 情報トラック
- 6 ブロック
- 7 データ
- 8 ディレクトリ
- 9 フォーマット情報
- 10 パスワード
- 31 光カード情報記録再生装置
- 32 ホストコンピュータ
- 33 MPU
- 34 AT／AF制御回路
- 38 光ビーム照射光学系
- 42 暗号化／復号化回路

【図2】

ファイル名 (12byte)
開始アドレス (2byte)
セクタ連続数 (2byte)
所定の数値 (2byte)

【図5】

セクタタイプ	セクタ数	セクタサイズ (バイト)
セクタタイプ1	1	1024
セクタタイプ2	2	512
セクタタイプ3	4	256
セクタタイプ4	6	128
セクタタイプ5	8	64
セクタタイプ6	12	32

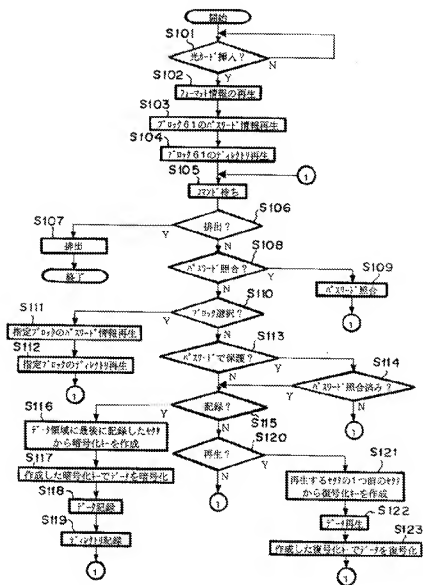
【図3】

ファイル名 (12byte)
開始アドレス (2byte)
セクタ連続数 (2byte)

【図6】

記録情報	アドレス 分教数	フォーマット セクタタイプ	フォーマット トラック情報	フォーマット セクタタイプ
------	-------------	------------------	------------------	------------------

【図1】



【図7】

【図9】

